Causal Factors of Increased Project Risk: A Review of Four In-Flight Anomalies

by

Rita M. Dal Santo

M.S. Space Systems, Florida Institute of Technology, 1994
B.S. Electrical Engineering, University of Florida, 1991

Submitted to the System Design and Management Program
in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology
[June 2006]
May 2006

Signature of Author _____

Rita M. Dal Santo
System Design and Management Program
May 2006

Certified by _____

Nancy Leveson
Thesis Supervisor
Professor of Aeronautics and Astronautics

Certified by _____

Patrick Hale
Director
System Design and Management Program

This page intentionally left blank

Casual Factors of Increased Project Risk: A Review of Four In-Flight Anomalies

by

Rita M. Dal Santo

Submitted to the System Design and Management Program in
Partial Fulfillment of the Requirements for the Degree of

Masters of Science in Engineering and Management

ABSTRACT

Risk management is an essential component any project. Traditional tools of risk management, however, tend to focus solely on the three traditional project elements—cost, schedule, and technical—ignoring the broader environmental issues which also play a part in project success. Without a knowledge and understanding of these additional factors, incident prevention is not possible. The thesis analyzes four in-flight anomalies to identify the underlying environmental factors that contributed to the technical failures.

The major themes found from the in-flight anomalies include the importance of a system perspective throughout the life of the project, the criticality of maintaining excellence during routine tasks, and the experimental nature of the projects.

Although nothing can guarantee a project success, research indicated the absence of key elements can set a project up for failure. These key elements include environmental awareness, proficient system engineering, engineering curiosity, engineering humility, and hands-on experience. Additionally, a cursory look at human and system behaviors that lead to resistance to change is provided.

Best practices and lessons learned from past incidents are provided and recommendations for future projects are suggested. A few of the recommendations are to establish a strong system engineering discipline, to provide hands-on training opportunities, and to improve current risk management practices to include system factors.

Thesis Supervisor: Nancy Leveson
Title: Professor of Aeronautics and Astronautics

Acknowledgements

I never would have applied for the MIT System Design and Management program if not for my NASA coworkers and management. Specifically, I would like to thank Cheryl McPhillips for encouraging me to apply for the fellowship; Larry Manfredi and Jon Cowart for helping me solidify my vision; Polly Gardiner for being the best sounding board ever; NASA SDM alumni Dawn Schaible, Keith Britton, John Stealey, and Tim Brady, for being *my* NASA cohort; and Tip Talone and Russell Romanella for providing me this once in a lifetime opportunity to expand my understanding of the complexities of the world.

To my fellow SDM classmates, your experiences helped me grow academically, professionally, and personally. Ram and Robin, thank you for the many philosophical conversations as we completed opportunity set after opportunity set.

To my advisor Nancy Leveson, your insight and patience helped me through a challenging second year. Thank you for your passion for system safety and teaching me to look beyond the obvious to the broader system issues.

To my parents, your enthusiasm throughout has been the best support I could have received. To my dad, who introduced me to the space program at an early age, I still remember visiting Ham at the museum and wondering why I could not see the men on the moon.

And, finally, to my husband, your support and assistance during our daughter's first year as I worked to finish my coursework and thesis made this possible. You have earned this degree as much as I have.

Table of Contents

List of Figures

Acronyms and Abbreviations

ASI	Agencia Spaziale Italiana (Italian Space Agency)
C&C	Command and Control
CIR	Cargo Integration Review
CORE	Shuttle Orbiter/Cargo Standard Interfaces, ICD2-19001
CRM	Continuous Risk Management
DDCU	Direct Current-to-Direct Current Converter Unit
DDHU	Digital Data Handling Unit
DRAM	Dynamic Random Access Memory
EMP	Enhanced Multiplexer/Demultiplexer
FEP	Fluorinated Ethylene Propylene
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
GN&C	Guidance Navigation and Control
HDRR	High Data Rate Recorder
HRDL	High Rate Data Link
ICD	Interface Control Document
IFA	In-Flight Anomaly
IFI	In-Flight Incident
IPR	Interim Problem Report
ISS	International Space Station
LaRC	Langley Research Center
LITE-1	Lidar In-Space Flight Experiment
JSC	Johnson Space Center
k	kilo
KSC	Kennedy Space Center
MDM	multiplexer/demultiplexer
MER	Mission Evaluation Room
MEIT	Multi-Element Integration Test
MIT	Massachusetts of Technology
MSD	Mass Storage Device
MSFC	Marshall Space Flight Center
N	newtons

NASA	National Aeronautics and Space Administration
NCS	Node Control Software
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OIU	Orbiter Interface Unit
OPF	Orbiter Processing Facility
PED	Payload Experiment Developer
PIRN	Payload Interface Revision Notice
PMA	Pressurized Mating Adapter
POCC	Payload Operations Control Center
PR	Problem Report
PRA	Probabilistic Risk Assessment
R&D	Research and Development
RAC	Risk Assessment Code
SCSI	Small Computer System Interface
SDM	System Design and Management
SFMDM	Smart Flexible Multiplexer/Demultiplexer
SRAM	Static Random Access Memory
SSMMU	Solid State Mass Memory Units
STS	Shuttle Transportation System
TSS-1	Tethered Satellite System
TSS-1R	Tethered Satellite System Reflight
US	United States
VDC	voltage, direct current
ZOE	Zone of Exclusion

Chapter 1: Introduction

1.1 Motivation

"To achieve success risk management must go far beyond corrective action prompted by incidents and accidents. All types of risk – including risk to human life – must be actively managed to achieve realistic and affordable goals."

- National Research Council report, September 2004 [19, pg. 15]

As the National Aeronautics and Space Administration (NASA) moves into the next phase of human exploration, all aspects of the agency must be realigned for success. Along with the technical challenges associated with spaceflight, political issues and organizational issues affect the agency's ability to pursue its goal of returning to the Moon and traveling beyond to Mars. The aging Space Shuttle fleet must be safely phased out and a new vehicle designed, built, and qualified, all in parallel with the completion of the International Space Station. Unmanned planetary missions and research satellite are also essential to support NASA's mission "to understand and protect our home planet, to explore the universe and search for life, to inspire the next generation of explorers… as only NASA can." Due to the perilous nature of spaceflight, risk management is an important factor in everything NASA does.

Risk consists not only of expected technical tradeoffs but is also associated with an organization's structure, management style, communication channels, and past successes and failures. In most large organizations, a project manager does not have control over every influence on a project; however, an effective project manager must still weigh the consequences of these factors when making decisions. The thesis will review four past in-flight anomalies in the hopes of providing insight into contributing factors that have the potential to increase system level risks of complex technical systems. Knowledge of

system level factors along with the ability to identify the impact of internal and external influences on overall project success will enhance the project manager's decision process.

1.2 Hypotheses and Objectives

The thesis proposes two hypotheses. The first hypothesis is that anomalies, mishaps, incidents, and accidents are often caused by emergent system factors not readily apparent when combined with issues of technical failure or human error. The second hypothesis is that traditional tools of risk management are narrowly focused on technical, schedule, and budgetary issues and do not provide a holistic view of the true risk of the project.

The first objective of the thesis is to review several well documented in-flight anomalies to determine the system level issues that contributed to the technical failure. Included in this review will be an examination of the risk management system employed by the project. For the second objective, causal factors that are common will be identified. As the third objective, recommendations for the implementation of a system safety approach to risk management as well as lessons learned will be provided for future projects.

1.3 Thesis Approach and Structure

The thesis draws from the experiences of past incidents, accidents and disasters to glean lessons of risk management for the everyday project manager. Along with cursory research into well-known accidents, three in-flight anomalies from the early 1990's Spacelab/Payload Program and one on-orbit anomaly from the International Space Station are examined for commonalities and underlying causes that led to the anomalies. Two of the four cases examined had post mission investigations including final investigation board reports. The other two had extensive post anomaly troubleshooting activities that were documented using the existing problem reports systems. Information not available through the existing documentation was obtained through personal interviews with individuals involved in the actual in-flight anomalies.

Chapter 2 frames risk management within the context of project management. Along with a discussion of the factors contributing to the risk of a project, a description of

NASA's continuous risk management program is provided. The perception of risk on a developmental project versus a production project is presented. Finally, a system dynamics approach to risk assessment is discussed.

Chapter 3 summarizes the four in-flight anomalies including background information on science and operational objectives. Findings from the official investigation board or from archived troubleshooting activities are summarized and an analysis of the system-level issues provided.

Chapter 4 offers the major and several minor themes found during the in-flight anomaly research and analysis. Examples of how these themes played out in the in-flight anomalies are given and other potential indications of the themes are discussed.

Chapter 5 provides lessons learned and recommendations. Key elements leading to project success are described. A cursory look at the question of why, even with the availability of lessons learned from past accident, incidents continue to happen is also provided.

Chapter 6 presents conclusions of the research and offers areas for future consideration.

Chapter 2: Overview of Risk Management Methodologies

"A program risk is any circumstance that poses a threat to crew or vehicle, safety, cost, schedule, or major objective."

W. Gerstenmaier [13]

"Project Management is Risk Management"

- overheard at NASA 2005 Risk Management Conference

2.1 Introduction

This chapter touches on several different approaches and ideas concerning risk management within a project. The traditional view of project management and where risk fits within this view is discussed. The NASA risk management policy guideline is reviewed and several tools available to the project are described. The environment of risk tolerance is discussed followed by an examination of the applicability of system dynamics to risk management.

2.2 Risk and Project Management

Project Management is "the application of knowledge, skills, tools, and techniques to project activities to meet project requirements." [30, pg. 6] Project success is determined by whether the project performs as expected and is delivered on time and within budget. Figure 1 is a classic representation of project management. Each project element is shown as the leg of an equilateral triangle that represents the equal importance and interdependence of each element to the success of the project. Project risks, existing in all areas of the project, are depicted by a circle in the center touching all three legs of the triangle.

Along with the risks inherent to technical projects, additional risks are incurred as tradeoffs are made to meet cost, schedule and technical requirements. Products are delivered with fewer features than originally promised in order to meet the release date.

Budget overruns occur in the effort to utilized cutting edge technology in an advance project. Schedule slips as problems occur in manufacturing or testing. Often it is performance that is sacrificed in order to meet an imposing deadline or a limited budget. Reduced technical ability does not necessary equate with project failure, but, as overruns occur, decisions begin to affect project risk. Successful risk management implementation allows the project to successfully trade requirements without impacting product sales or, in more serious circumstances, compromising project safety.

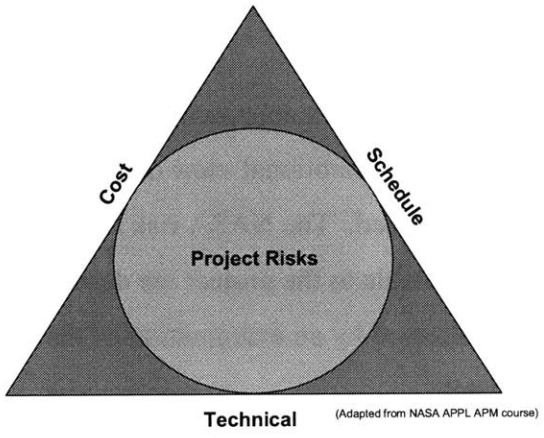

Figure 1: Traditional Project Management Triangle [3]

2.3 Risk As A Function

Geveden [14] provides a different approach for considering project risk. (see Figure 2) In this model, risk is viewed as a function of cost, schedule, and performance. The level of project risk changes as the other elements are held "constant." In other words, as the project manager manages cost, schedule, and performance, the overall project risk responds accordingly.

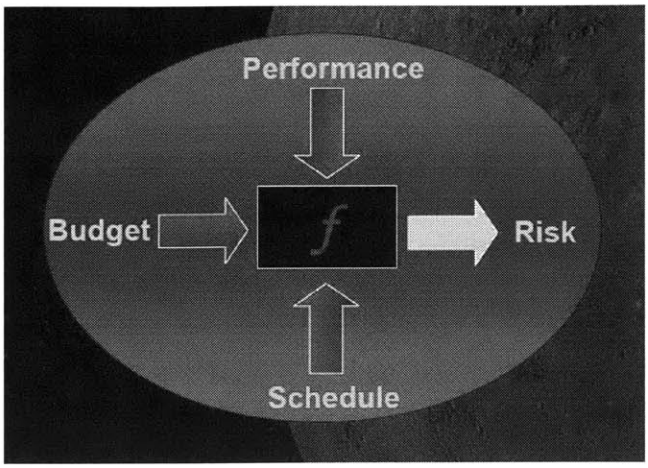

Figure 2: Typical Project View of Risk [14]

The model can be tailored to accurately portray unique project circumstances. If the project is not willing to increase risk and has the ability to allow a different project element to vary, then risk becomes an input to the function and the other element becomes the output. For example, in the post-Columbia environment (Figure 3), the "return to flight" mission was not cleared to launch until the foam shedding problem on the external tank was understood and resolved. No additional budget was allocated and, therefore, the launch date continued slip until the program believed it was safe to fly. [14]

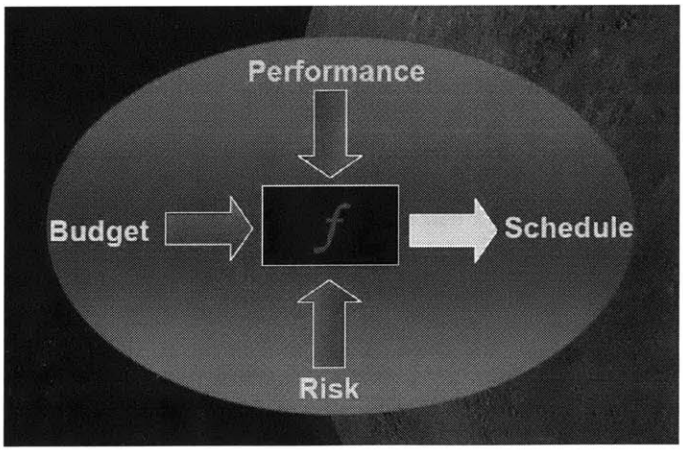

Figure 3: Project View of Risk (Post Columbia) [14]

The model also lends itself to the inclusion of the other less tangible elements affecting risk. Figure 4 represents the model that considers environmental elements. Environment elements for NASA include [14]:

- political (e.g., presidential direction, congressional budget considerations)
- policy (e.g., agency governance, agency directives)
- strategy (e.g., international partnerships)
- architecture (e.g., orbiter glider vs. manned capsule vehicle design)
- culture (e.g., leadership styles, communication channels)
- functional (e.g., manufacturing processes, project control gates)

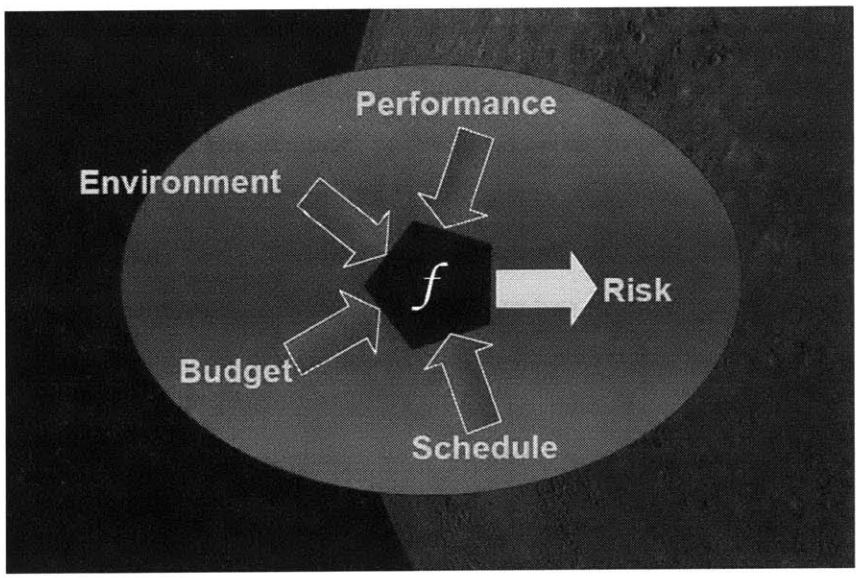

Figure 4: Fourth Dimension of Risk [14]

2.4 Risk Management at NASA

NASA Procedural Requirement Risk Management Procedures and Guidelines (NPR 8000.4) defines Risk Management as "a process wherein the program/project team is responsible for identifying, analyzing, planning, tracking, controlling, and communicating effectively the risks (and the steps being taken to handle them) both

within the team and with management and stakeholders." [27] The continuous risk management (CRM) philosophy adopted by NASA and pictorially represented in Figure 5 captures the belief that risk management is an iterative process that spans the entire life of the project.

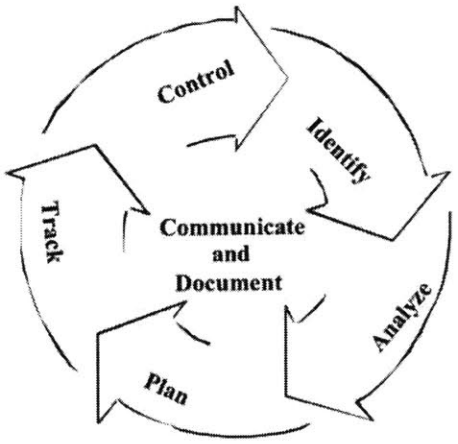

Figure 5: NASA Continuous Risk Management [27]

Initially, the project must *identify* the risks including not only what can go wrong but also what is the consequence if the risk occurs. *Analysis* encompasses the determination of the likelihood of the risk occurring, the time frame in which action is required to prevent the risk, and a relative scale rating how this risk compares to others. Next, the project must *plan* what preventative actions (if any) should be taken for each risk. The project can mitigate, accept, research, or monitor the risk. *Tracking* is used to determine how well the risk management plan is performing. *Control* is used to reevaluate the current risk plan and make necessary changes as the project evolves throughout its life cycle. Central to the success of CRM is the need for the project to *communicate and document* during each phase. Each project is required by NASA to have an official risk plan document. [27]

NPR 8000.4 lists several useful tools available for each phase of the risk management plan. For the *identify* phase, system safety and reliability analyses (e.g., hazard analysis, fault tree analysis (FTA), failure modes and effects analysis (FMEA)), simulations, and

models are mentioned. Probabilistic risk assessment (PRA), uncertainty analysis, FTA, and FMEA are useful for the *analyze* phase, as well as the Risk Assessment Code (RAC). Cost-benefit analysis, PRA, and risk plans and lists are needed for the *plan* phase. No specific tools are mentioned for *tracking* or for *communicate and document*. NPR 8000.4 stresses the use of team member experiences, lessons learned, historical data, review boards, and test and analysis data as valuable resources for input to each phase of the continuous risk management process. [27]

NASA has adopted the use of the RAC via the risk matrix as a primary tool to aid risk management. The risk matrix shows the probability and effect of an event occurring. Consequence is defined as "an assessment of the worst credible potential results(s) of a risk" [27] and is classified as catastrophic, critical, moderate, or negligible. Likelihood is defined as "the probability that an identified risk event will occur" [27] and is ranked from highly likely to improbable. NPR 8000.4 provides a guideline for rating consequence and likelihood and allows for each project to tailor the levels to meet the unique project circumstances. In all cases, the most risky events are classified as highly likely and of high consequence. Figure 6 is a representation of the risk matrix.

	LIKELIHOOD ESTIMATE				
CONSEQUENCE CLASS	A	B	C	D	E
I	1	1	2	3	4
II	1	2	3	4	5
III	2	3	4	5	6
IV	3	4	5	6	7

High Risk	
Medium Risk	
Low Risk	

Figure 6: Risk Matrix Showing Risk Assessment Codes [27]

The risk matrix is a useful tool to communicate risks across the project. The matrix is not limited to technical risks. Budget and schedule impacts can also be addressed, though

correlation between impacts of budget, schedule, and technical risks can be difficult. It is important to remember the matrix only accounts for risks that have been identified. Undocumented or unknown risks are not accounted for since the risk must be visible to be ranked. Additionally, normal implementation of the risk matrix identifies risks by engineering discipline (e.g., electrical, mechanical), operational condition (e.g., design, manufacturing, testing) or project element (e.g., technical, cost, schedule); therefore, system-level risks are often missed.

2.5 Environment of Risk Tolerance

Project success can be affected by the different risk tolerance level among stakeholders. Engineers often have a low tolerance for technical risk, believing technical excellence should not be compromised for schedule or budget concerns. On the other hand, project managers tend to have a higher tolerance to technical risk since they also must weigh the political ramification of a cost overrun or schedule slip. [2] Even when the public seems to accept high technical risk, their tolerance for human injury or loss of human life is next to none. Clearly, accurately portraying all risks associate with a project and gauging the stakeholder tolerance of those risks is an essential part of risk management.

Taylor [33] states approaches and tolerances to risk in the corporate and public arena depend on whether the project is classified as research and development (R&D) or as product development. Figure 7 represents the risk tolerance environment for different project types. During the R&D phase, a project is using corporate "risk money" and a higher tolerance for failure exists. R&D is seen as a learning experience and companies do not necessarily expect a direct return on investment. In contrast, during product development, a project is using corporate "budget plan" money, the company expects a direct return on their investment, and project managers' careers are made or broken with project success or failure. Any mismatch between the true nature of a project and classification of the project will result in a discrepancy between the expected and actual outcome.

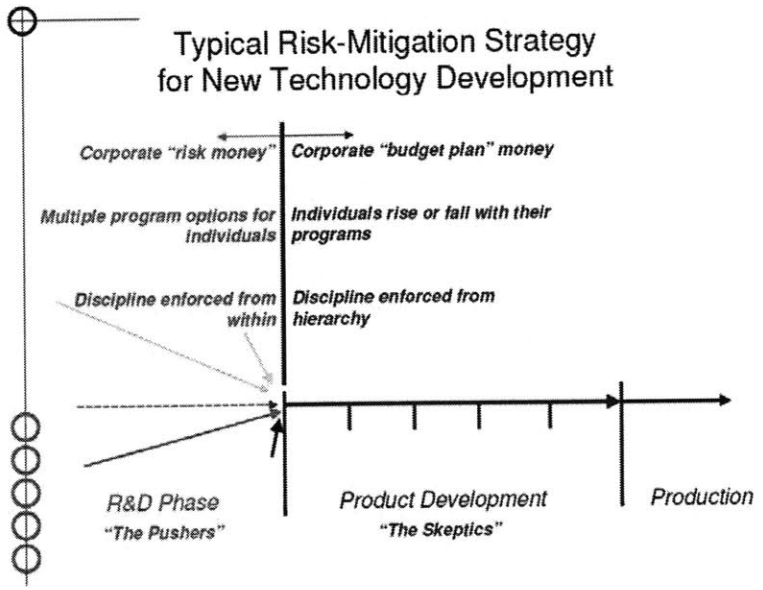

Figure 7: Environment of Risk Tolerance for R&D and Product Development [33]

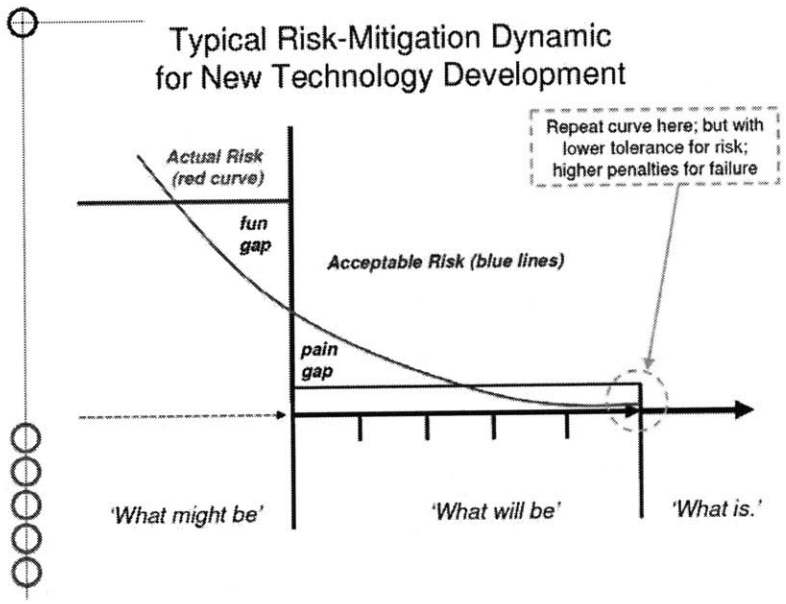

Figure 8: Actual and Acceptable Risk for R&D and Product Development [33]

As shown in Figure 8, the acceptable risk of a project is a step function, dropping significantly at the R&D/product development line. The actual risk follows a parabolic curve which decreases as the project moves from R&D, through product development,

and into production. Two areas of discrepancy exist between the level of actual risk and the level of the acceptable risk. When the actual risk is lower than the acceptable risk, the project is in the fun gap and has room to manage unexpected risks. When the actual risk is higher than the acceptable risk, the project is in the pain gap and must work diligently to reduce the probability of risks from becoming reality. It is within this pain gap that many of NASA's projects operate.

2.6 System Dynamics Approach to Risk Management

Traditional tools used for risk management do not readily address the system aspects of a project, often ignoring the environmental elements that affect risk. The field of system dynamics, developed by Jay Forrester in the 1950s, is applicable to system-level risk management. System Dynamics utilizes feedback control theory and the theory of nonlinear dynamics to study the complex interactions of different aspects of a system. [31] It relies on the principle of systems thinking—"the ability to see the world as a complex system, in which we understand that 'you can't just do one thing' and that 'everything is connected to everything else'" [31, pg. 4] and provides "a framework for dealing with dynamic complexity where cause and effect are not obviously related." [18, pg. 9] It not only looks at the traditional elements of a project—cost, schedule, technical—but considers human behavior, external pressures, cognitive and social psychology, economics, and other social sciences.

2.6.1 System Dynamics Model Description

The typical system dynamics model consists of system variables linked together by positive and negative feedback control loops. Positive feedback loops reinforce behavior (and are thus called reinforcing loops). Negative feedback loops counteract behavior (and are thus called balancing loops). Arrows are used to show influence among variables and the relationship between variables is indicated by a plus or minus sign. A positive relationship (indicated by a plus sign) means the variables will respond in the same manner (i.e., if X increases then Y will increase) and a negative relationship (indicated by a minus sign) means the variables will behave in a manner opposite to each other (i.e., if X increases then Y will decrease).

An important benefit of system dynamics models is the ability to include time delays between a change in stimulus and the response of the system. While the effects of short time delays might be relatively easy to anticipate, system complexity makes it almost impossible to predict the effects of a long time delay. Without the aid of an effective model, "decision makers often continue to intervene to correct apparent discrepancies between the desired and actual state of the system even after sufficient corrective actions have been taken to restore the system to equilibrium." [31, pg. 23]

2.6.2 System Dynamics and System Safety Research at MIT

Massachusetts of Technology (MIT) researchers has recently developed a system dynamics model to assess system safety. "A sophisticated system model of the engineering and safety culture at NASA to better understand and characterized the cultural and socio-political aspects of risk" [12, pg.10] was developed by Leveson, et. al., as a result of the safety culture issues identified during the Columbia Accident Investigation Board. Figure 9 is a simplified model of the factors related to the Columbia accident.

In the center of the model is a large balancing loop labeled *Limits to Success (B1)* and within that loop are a smaller balancing loop, *Problems have been fixed (B2)*, and reinforcing loop, *Pushing the Limit (R1)*. Starting with the system safety variables in the upper right corner of loop *B1*, the model shows as *budget cuts* increase, *budget cuts directs towards safety* increase, and *system safety efforts* in turn decrease. Also influencing system safety, as *performance pressure* increases, *priority of safety programs* decreases and *system safety efforts* decrease. In the upper right corner, Loop *B2* shows how as *perceived safety* increases, *complacency* increases, and, eventually, *system safety efforts* decreases. The decrease in *system safety efforts* leads to a decrease in actual *safety* and eventually an increase in *risk*. An increase in *risk* results in an increase in *accident rate*. The model also includes the influence of *performance pressure* (Loop *R1*) on the system safety.

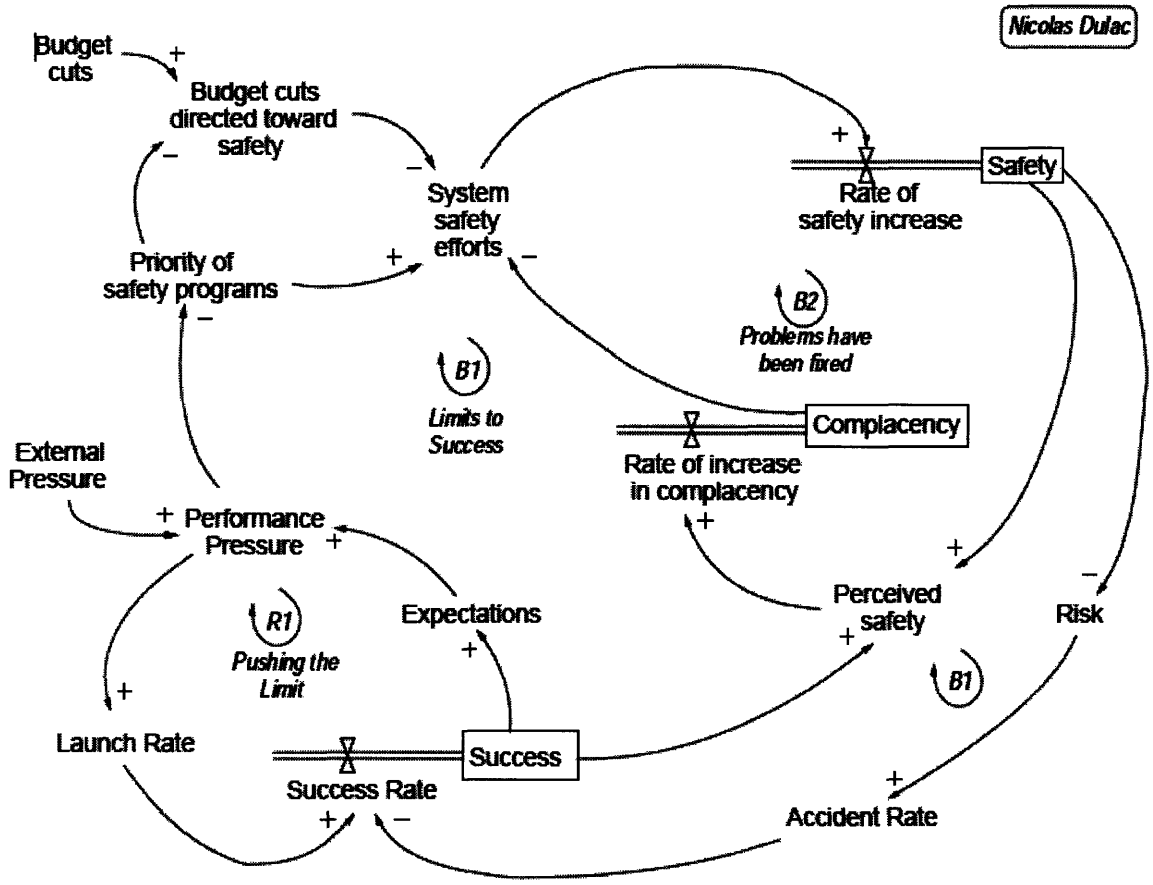

Figure 9: Simplified Model of System Dynamics of Space Shuttle Columbia Accident (Leveson & Dulac) [18]

Other research at MIT has used system dynamics to create an accident model [17] which, instead of looking at root causes of accidents, examines the reasons behind why pre-existing control systems were not able to prevent accidents. A system dynamics model has also been used to assess the risks associated with a new NASA organizational structure established to give technical concerns equal weight with programmatic concerns. [19] Research has also developed a user-friendly risk management simulator to allow NASA project managers to "explore the dynamics of risk using an advance system dynamics simulation of the NASA safety culture prior to the Columbia Shuttle accident." [12, pg. 2]

Chapter 3: Analysis of In-Flight Anomalies

"Failure is one of the products of exploratory development."

- TSS-1R Investigation Board [32, pg. 4-3]

3.1 Introduction

This section analyzes four in-flight anomalies from NASA's human spaceflight program. Three examples are from the Spacelab/Payloads Program and one is from the International Space Station (ISS) Program. The risk management approach of each project appeared sufficient (at the time) to manage the anticipated difficulty yet each flight experienced a significant anomaly. In each case, a technical cause was found but further analysis uncovered additional contributing factors. Only the ISS in-flight anomaly had potential to seriously impact crew safety; however, all significantly impacted mission operations and to an extent mission success.

3.2 Spacelab/Payloads In-Flight Anomalies

The Spacelab/Payload Program ran from 1981 to 1998 and was one of NASA's most successful programs. Throughout the course of 28 missions [7], over 750 life and microgravity science experiments [29] were performed in the Spacelab module or on carriers housed in the Space Shuttle payload bay. Three of the in-flight anomalies examined for the thesis occurred during this time period: the Tethered Satellite System, the Tethered Satellite System Reflight, and the Lidar In-Space Technology Experiment.

3.2.1 Tethered Satellite System Mission

3.2.1.1 Tethered Satellite System Mission In-Flight Anomalies

The Tethered Satellite System (TSS-1), a joint project between the Italian Space Agency (Agenzia Spaziale Italiana - ASI) and NASA, attempted to verify the feasibility of tethers in space. Mission objectives were "to evaluate the capability for deploying, controlling and retrieving a tethered satellite; to validate predications of the dynamic forces at work in a tethered satellite system; to conduct exploratory electrodynamics science

investigations; and to demonstrate the capability of the system to serve as a facility for research in the geophysical and space physics." [1, pg. 7] The payload consisted of the satellite, the deployer system, the tether, several science experiments, and the carrier hardware and associated subsystems. The tether and deployer systems were designed to allow for the satellite to be deployed 20 kilometers. Science experiments were housed inside the satellite and also on the carrier pallet in the shuttle payload bay.

Marshall Space Flight Center (MSFC) had overall project management responsibility for the integrated payload and also provided the carrier and associated hardware. Alenia in Torino, Italy, designed and developed the satellite under contract to ASI. Martin Marietta in Denver designed and developed the deployer system. The tether was manufactured by Cortland Cable Company. The science experiments were developed by various universities and government agencies.

The TSS-1 program was concluded before NASA adopted the current risk management approach requiring an official risk management document and the use of the risk matrix. Instead, the project manager kept a list of "leans and threats" addressing the technical, schedule, and cost implications of potential negative outcomes. [10]

TSS-1 underwent normal Kennedy Space Center (KSC) pre-flight processing operations. The flight tether was loaded onto the deployer reel in September 1991. A flight tether motion test was conducted in October 1991 during which approximately 30 meters of tether was deployed and retrieved. A complete deployment and retrieval of the tether was not possible during KSC ground processing activities due to the handling limitations of a one-g environment. In early 1992, after the Shuttle Program loads analysis identified a negative margin of safety, a modification to the deployer system was performed to increase the structural integrity of the reel support structure fasteners. No additional tether deployment was performed after the modification. [1]

TSS-1 flew aboard STS-46 in the summer of 1992. During satellite deployment, the payload operations team encountered five anomalies: (1) failure of the U2 connector to

disengage; (2) initial failure of the satellite to fly away; (3) tether deployment failure at 179 meters; (4) tether deployment failure at 256 meters, and (5) tether deployment failure at 224 meters. [1]

The U2 umbilical initially failed to separate from the satellite when commanded. Ten more separation attempts were made utilizing a variety of techniques. Finally on the twelfth attempt, which included "relieving tether tension, pulsing the umbilical motor, and firing the Orbiter thrusters to maneuver the Orbiter away from the satellite" [21, pg. 9], the connector separated and the mission was able to proceed. Post-mission investigation was inconclusive as to why the U2 umbilical had difficulty separating. Potential contributing factors include the fact that pre-flight separation testing did not completely simulate the U2 flight hardware configuration and that the pin assemblies exceeded drawing specifications for pin protrusions. Additionally, a slight adjustment to the connector pins had occurred after thermal vacuum tests were completed and re-test was not performed. [1] For future missions, the U2 umbilical was removed and critical functions moved to the U1 umbilical. Additionally, the U1 umbilical motor pull force was increased to allow for additional margin in the separation capability. [21]

The inability of the satellite to deploy during initial flyaway and also the failure to deploy at the 224 meter distance was determined to be caused by the tether jamming in the deployer tether control mechanism. Post-mission investigation found the tether jam anomaly to be caused by four factors: existence of tether slack, the vernier motor accelerating the tether in the control mechanism faster than it could be pushed out, the stiffness of the tether eyesplice used to secure the tether to the satellite, and ground testing not accurately simulating the acceleration of the satellite in zero-g. To correct the tether jam problem on future flights, several design and operational changes were required. The vernier motor was modified to allow for a gradual application of force to the tether. The eyesplice was shortened at the tether end. Changes to the operational sequence of deployment were incorporated for subsequent missions. And, finally, future ground testing was improved to more accurately simulate satellite acceleration during fly-away. [21]

The tether stops at 170 meters and 256 meters were found to be caused by mechanical interference in the level wind. Specifically, a bolt used to install a wedge block late in the ground flight processing flow protruded into the path of the tether and stopped the tether from deploying past the 256 meter point. The wedge block was added to the deployer system after stress analysis indicated a violation of the allowable margin. Post installation testing to check for interference was not performed. For future missions, the wedge block bolt was modified to remove the interference. [21]

3.2.1.2 TSS-1 In-Flight Anomalies Causal Factors

The TSS-1 Post-Mission Investigation Board stated the primary causes of the in-flight anomalies were as follows [1]:

- The protruding bolt created interference with the level wind travel causing the tether stops at 179 and 256 meters.
- Tether slack followed by excessive tether acceleration by the vernier motor causing the tether to bind was the most probable reason for the initial failure to flyway and the failure to move the tether in either direction at 224 meters.
- No conclusive findings were found for the most probable cause of the U2 separation failure.

The investigation board declared "flight hardware changes incurred late in the project cycle (in particular after completion of systems test) are at best a high risk undertaking." [1, pg. 45] The mechanical interference with the bolt on the wedge block would have been discovered if a tether deployment test had been performed after the modification. Sufficient retest of the deployer system would have been difficult with the facilities available at KSC and schedule pressure prevented shipping the system back to the design facility for retest.

The addition of the wedge block was in response to stress analysis results showing negative safety margin in the front reel foot to reel support structure fasteners. Instead of being discovered by the payload loads analysis process, which occurs much earlier in the

life of a mission, this negative margin was not discovered until the shuttle loads analysis, much later in the mission flow. The preferred solution to install larger fasteners would have required significant de-integration of the payload. Reperformance of the carrier to deployer integration testing would have required shipment back to the design facility. The time needed to de-integration, re-integration, and retest would have resulted in a launch delay and therefore this solution was rejected. Instead the wedge block solution was implemented. Unfortunately, the potential for interference was not identified or realized. No retest was performed. Post-mission investigation showed the existing drawings did not match the as-built configuration and also did not provide the right view to show the interference. [1]

The post-flight investigation board stated "the ... process appears to have had a narrow structural mod[ification] perspective without adequate systems level assessment (e.g. potential for the modification to intrude into the dynamic envelop of the level-wind mechanism translation travel)." [1, pg. 42] A previous indication of inadequate system level perspective was evident in an earlier carrier modification that required a change to the attachment of the thermal subsystem component. The significance of this structural design modification was not recognized by the carrier organization, the satellite organization, or the payload engineering organizations. [1] This change lead to the negative safety margin, the late hardware modification, and, ultimately, the in-flight anomaly.

The potential for slack in the tether was known to exist but the conditions under which tether slack would occur were not fully appreciated. [1] The board questioned the effectiveness of the ground testing program to adequately explore the operational environment especially for specific sensitive parameters such as tether slack. The board believed the fact that there was limited off-nominal testing contributed to the lack of understanding of the potential and consequences of tether slack. Flight hardware is not normally utilized to perform off-nominal testing and no extra hardware existed. If off-nominal testing had occurred, the project might have been better prepared to handle the unexpected operational scenarios encountered during the mission.

3.2.2 Tethered Satellite System Reflight Mission

3.2.2.1 Tethered Satellite System Reflight Mission Tether Separation In-Flight Anomaly

The Tethered Satellite System Reflight (TSS-1R) mission was a reflight of the TSS-1 mission. During the earlier mission, the satellite had failed to deploy past the 256 meter distance due to mechanism problems. The primary goal of the reflight mission was to meet the objectives not met by TSS-1. (These objectives are listed in Section 3.2.1.1) For the reflight mission, the payload had been modified based on the TSS-1 post mission investigation board findings and recommendations. MSFC retained mission management responsibilities. As with TSS-1, risk management consisted of a list of "leans and threats" addressing the technical, schedule, and cost implications of potential negative outcomes. [10]

A brief description of the tether is relevant. The electrically conductive tether consisted of five layers. A ten 34 gauge wire helix twist copper conductor surrounded the innermost layer, a Nomex core. Fluorinated Ethylene Propylene (FEP) insulation covered the conductor/core combination. On top of the insulation, braided Kevlar provided the tether strength. The outside layer, a Nomex braid, protected the tether from atomic oxygen and abrasion. All together the tether measured 2.54 millimeters thick. It had a rated breakstrength of 1780 newtons and was designed to handle a 15 kVDC potential (qualified to 10 kVDC). The tether was qualified to carry 2.5 amperes for 20 minutes. [32]

After the TSS-1 mission and before the reflight mission, the 300 meters of tether deployed during TSS-1 was removed and tested to determine the effects of the space environment on the tether. No significant degradation was found. Recommended modifications to the deployer system were performed after which two full tether deploy/retrieve cycles were performed. A high voltage instrumentation test occurred in June 1995. Final mating of the tether to the satellite happened in August 1995 after the

pin was reworked due to poor connectivity. No tether problems were uncovered during the follow-on ground testing of the payload system. [32]

TSS-1R flew aboard STS-75 on February 22, 1996. Tether deployment began on day 3 of the mission. No significant tether problems were encountered until approximate 5 hours into satellite deployment when the tether broke with 19.7 kilometers extended, 1 kilometer from the final deployment length. The satellite and tether were lost and eventually burned up in the upper atmosphere. [32]

Post-flight inspection showed the tether end to be charred. The few strands of Kevlar that remained at the end of the tether also showed indications of tensile failure. Evidence of arcing existed within the deployer mechanisms. Additional inspection of the deployer discovered very fine silver plated wire, aluminum shavings, small metallic shavings, and unidentified non-metallic debris. Inspection of the remaining tether found metallic and non-metallic contamination within the tether insulation. Damaged strands within the copper conductor were discovered during post-mission investigation testing. [32]

At the time of breakage, the load on the tether was believed to be 65 newtons. It was carrying a current of 1 ampere and a voltage potential of -3500 VDC with respect to orbiter ground. [32] These values were well within the operating parameters of the tether. Without the arcing and subsequent burning of the Kevlar sleeving, the tether would have successfully deployed to its final length and the experiments continued.

The in-flight anomaly was not easily duplicated; therefore, the investigation board spent significant time and effort to determine the cause. Arcing was obvious but what initiated the arcing was not. Post-mission testing was unable to create an arc using undamaged tether. Additional analysis of the compression forces within the deployer reel were needed to show debris could be forced into the tether insulation and create a small hole. Such a pinhole was suspected to have caused an electromagnetic breach, resulting in arcing from the tether conductor to the deployer mechanisms. Arcing continued within deployer mechanism until the pinhole reached the plasma of space. Plasma fueled the

arcing, which in turn allowed the tether to burn. Once enough tether had burned away, the Kevlar braid experienced a tensile failure which resulted in the tether breaking and, thus, the satellite separating. [32]

The science experiments provided critical data invaluable to the investigation board in determining the conditions and sequence of events just before the tether broke. Interestingly the data were almost not available at the time. A subsystem computer kept reinitiating itself due to an unknown condition. With each reset, the data link to the science experiments was lost. Because of safety concerns, the flight director had decided, if the subsystem computer experienced a reset during deployment operations, science experiment recovery efforts would have to wait until after completion of tether deployment. Luckily no reset occurred and the experiments were on-line at the time of satellite separation. In addition to the invaluable insight into the events leading to tether separation, the data collected by the science experiments during tether deployment and even after tether separation were unique in the field of plasma physics.

3.2.2.2 TSS-1R In-Flight Anomaly Causal Factors

The TSS-1R Post-Mission Investigation Board stated the primary causes of the in-flight anomaly as [32, pg. 4-1, 4-2]:

- "The tether failed in tensile under nominal loads due to the degradation of the Kevlar strength member by arcing and burning."
- "External foreign object penetration, or a defect in the tether, caused a breach in the FEP insulation layer, resulting in arcing."

Cortland Cable Company had extensive experience manufacturing both mechanical and electromechanical tethers. Kelvar lines had been used for satellite and balloon mechanical tethers up to 100 kilometer. Cortland utilized Kevlar and a special conductor core for electromechanical tethers used in undersea sonobuoys. The TSS tether was based on a Navy application during which the tether was exposed to thermal expansion and contraction as well as rapid changes in tension. Both conditions were likely on the TSS mission. Specific fabrication procedures were developed to effectively integrate the

conductor, insulator, and strength layers while protecting the TSS tether from undue stress. Inspection and test were integrated into the fabrication process so defects could be repaired as they occurred. Upon completion, acceptance testing was performed to verify proper workmanship. [32]

TSS was the first use of an electromechanical tether in space. It was truly an experiment. Experience with electromechanical tethers in naval applications, while providing some level of confidence, did not address the unique concerns of operating a conducting tether in the environment of space. The close proximity of the tether to the deployer mechanisms and thus the orbiter ground created a situation that was dependent on the integrity of insulation. The significance of a manufacturing defect in the insulation (such as a pinhole) was appreciated and care was taken to insure defects were corrected before integration with the deployer system. [32]

In spite of the special fabrication procedures, the board believed the vulnerability of the tether insulation was not fully appreciated as was evident by less stringent fabrication and test process requirements. The TSS tether was fabricated under normal shop conditions and was exposed to the associated level of debris and contamination. None of the extra precautions normal for components sensitive to contamination during space applications (such as utilizing a cleanroom) were taken and the manufacturing environment was not listed in the Failure Modes and Effects Analysis (FMEA). Contributing to the lack of awareness of the insulation vulnerability was the limited understanding of compression forces on the tether associated with deployer spooling operations. Appreciation for the ease at which compressions forces could push a small piece of debris through the braiding and into the insulation did not exist before the mission. [32]

As was previously mentioned, TSS was a complex mission. Because of the interdependence of the tether, deployer, science experiments, and orbiter, an integrated system engineering approach was critical for mission success. A holistic perspective from requirements development, through design, fabrication, and testing, to operations was critical in managing the integrated system aspects of the project. For example, the

board believed the tether and the deployer system should have been designed in concert to avoid concerns of winding forces effects on the tether. [32] Yet, the systems were designed and manufactured separately. As a result, high sensitivity to debris in the deployer system did not exist and (as mentioned above) susceptibility of the tether insulation to damage from such debris was not appreciated.

3.2.3 Lidar In-Space Technology Experiment Mission

3.2.3.1 Lidar In-Space Technology Experiment High Data Rate Recorder In-Flight Anomaly

The Lidar In-Space Technology Experiment (LITE-1) was a Langley Research Center (LaRC) managed research and technology experiment which flew on STS-64 in September 1994. The experiment consisted of a class IV laser operating at three wavelengths. The laser was directed into the Earth's upper atmosphere and data were acquired to measure "stratospheric and tropospheric aerosols, cloud formation altitude and thickness, atmospheric temperature and density, and the planetary boundary layer." [16, pg. 1-1] The experiment also tested the feasibility of operating a powerful laser in a vacuum as well as provided an understanding of the engineering requirements necessary to successfully operate a spacebased lidar system. Correlated data using ground and airbased remote sensing systems were collected throughout the mission. LITE-1 experienced several on-orbit anomalies; however, "all of the objectives of the LITE payload were accomplished and in some cases exceeded." [16, pg. 1-1] This research will concentrate on an anomaly with the High Data Rate Recorder (HDRR).

Johnson Space Center (JSC) had responsibility for overall mission management including the other payloads flying on STS-64. Payload operations were conducted out of the JSC Payload Operations Control Center (POCC) located across the hall from the Space Shuttle Mission Control Center. LaRC maintained management of the LITE payload including payload mission operations. The LaRC payload development and science teams were involved throughout the entire project management cycle and actively

participated in KSC ground processing activities, shuttle/payload reviews, and flight readiness reviews.

The LITE mission flew before the current NASA risk management practice of an official risk management document and adoption of the risk matrix. The project manager maintained a list of top risks and potential threats to the project plan, which were discussed at weekly status meetings. [8]

MSFC provided the Spacelab Enhanced Multiplexer/ Demultiplexer Pallet (EMP) pallet on which LITE was physically mounted. MSFC also provided the Smart Flexible Multiplexer/Demultiplexer (SFMDM) control computer and the HDRR. The HDRR would record science data during data takes. Data recorded on the HDRR would be downlinked when ground communication via the orbiter KU-Band antenna was available. JSC provided the remaining integration hardware including the connecting cables between the LITE/EMP/subsystem payload and the space shuttle orbiter (where the HDRR was mounted in the aft-flight deck).

LITE underwent normal KSC integration and test activities including post-delivery atmospheric testing, pre-orbiter interface testing, and orbiter interface verification testing in the Orbiter Processing Facility (OPF) and at the launch pad. All problems encountered during ground processing were understood and either resolved or accepted for flight. (One exception was the SFMDM "warm-start" issue which is out of scope of the research for this thesis.) Ground testing between LITE and the HDRR was performed in a flight-like configuration and no significant problems were found.

Early in the LITE mission, the LaRC POCC team was unable to playback data from the HDRR. On-orbit troubleshooting indicated the playback data did not contain valid frame sync patterns. [16] The problem was not correctable on-orbit. A significant replanning effort was performed to utilize the orbiter downlinked capability to record the real time data on the ground and guard against the possible loss of science data. This effort

required additional personnel for replanning and also required the key scientists to work extended shifts over the length of the mission. [16]

After the mission, extensive troubleshooting was performed at KSC to isolate the problem. A 40 foot delta was found to exist between the differential data record pairs (Record Data, Record Clock Not) in the orbiter flight cables which connected LITE in the payload bay to the HDRR in the aft flight desk. This large delta in cable length essentially cancelled the ability of the differential lines to invert the noise and add it to the real signal. Instead, the existing noise was potentially doubled overriding the existing true signal and making it unreadable. [25] The cable length delta did not completely explain the in-flight anomaly however since it was present in the pre-flight test configurations. Further analysis showed post flight troubleshooting recreated the anomaly when the payload was operated without cooling where as pre-flight testing was performed with payload cooling. It was believed the lack of payload cooling allowed post-flight troubleshooting to better simulate flight-like temperatures. [25]

3.2.3.2 LITE-1 In-Flight Anomaly Causal Factors

The post-flight troubleshooting problem report was closed as an unexplained anomaly with the most probable cause being "cable length deltas between clock record pairs and data record pairs. These cable length deltas in combination with nominal on-orbit temperature of the DDHU [Digital Data Handling Unit, a subsystem on LITE] and/or nominal fluctuations of electronic components in the DDHU could have caused the anomaly." [25, pg. 98]

During post-flight troubleshooting, it was determined the cable length delta was not part of the original flight configuration. A cable harness that ran between the LITE payload and the HDRR was switched out by shuttle design avionics after the Cargo Integration Review (CIR) had occurred. No documented evidence could be found stating why the cable harness was changed. A KSC payload engineer suggested the possibility that additional cable length might have been needed for routing purposes. [9] The LaRC

payload experiment developer (PED) was not informed of the change at the time it occurred.

KSC payload engineering became aware of the cable length delta when developing the test configuration for pre-flight testing. The standard drawings used to develop test configurations were low fidelity and did not provide certain details such as actual cable lengths. Higher fidelity drawings were requested for an unrelated reason. With the new drawings, the delta on the differential lines was noticed by a KSC payload engineer. The engineer was concerned about the potential impact of a cable delta and spoke with the LITE PED but the LITE PED did not seem to share the concern. In hindsight, the KSC payload engineer believes he did not effectively communicate his concern to the LITE PED. [9] The LITE PED has no recollection of a cable length delta discussion with the KSC engineer before the mission. [8]

The reason behind the decision to use differential data record pairs for the HDRR interface could not be found within the available shuttle/payload documentation; therefore, shuttle design avionics potentially had no knowledge of the importance of equal cable lengths for this particular interface. Swapping the original cable harness for a harness with different lengths made sense if indeed more length for routing purposes was needed. The Shuttle and Payloads Programs operated independently of each other with limited communication between the two. Communication was strictly through formal documents and reviews. There was very little personal interaction between the two programs. A system integration role did not exist to look across the shuttle/payload interface for design issues.

As a corrective action, the problem report stated "shuttle design avionics would be required to generate a PIRN [Payload Interface Revision Notice] to the CORE ICD [Interface Control Document; ICD2-19001 Shuttle Orbiter/Cargo Standard Interfaces] to preclude large cable length delta associated with this type of interface." [25, pg. 98] It is surprising this was not normal practice at the time, though perhaps the shuttle/payload culture of the time can explain this oversight. The Shuttle Program operated under the

mode that it provided a standard set of services within specific specification to the payload customers. The payload customers were expected to design to operate within the shuttle parameters. Any changes interior to the shuttle should not affect payload operations and, therefore, the payload did not need to be informed when changes were made. One can speculate shuttle design avionics incorrectly assumed the cable harness change was benign and therefore it was unnecessary to inform the payload developer.

While a standardized interface approach is necessary for a program that provides a particular service to a multitude of customers, awareness of how changes might affect the customer is still important so the customer can plan and act accordingly. The Shuttle/Payload Program culture, however, did not promote collaborative exchange between orbiter and payloads. This was not an isolated instance and it was often joked that the shuttle would fly whether the payload was ready or not. LITE actually experienced another occurrence of a shuttle change affecting payload operation. During orbiter verification testing, the orbiter coolant temperature was changed unknown to the broader test team. Shortly afterwards, unexpected data for a component of LITE were noticed and a payload problem report was opened. Troubleshooting finally uncovered a change in temperature caused the erratic behavior. Even then, shuttle was reluctant to provide the exact temperature data. As they told the team, the payload was supposed to be able to operate at whatever temperature the shuttle provided; therefore, the exact temperature was irrelevant. While the payload did have to live with the shuttle thermal output, the change in temperature did have an affect on the payload and the payload needed to know the information so they could compensate.

3.3 International Space Station On-Orbit Anomaly

The first element of the International Space Station (ISS) was the Russian Control Module, Zarya. Its launch in November 1998 was followed shortly by the first United States (US) elements. The fourth in-flight anomaly examined in the thesis is an on-orbit anomaly from the 6A assembly mission.

3.3.1 ISS Flight 6A Mission

3.3.1.1 ISS Flight 6A Command & Control Computer On-Orbit Anomaly

ISS assembly mission 2A consisting of Node 1 and two Pressurized Mating Adapters (PMA) was launched in December 1998 aboard STS-88. Node 1 housed two multiplexer/demultiplexer (MDM) control computers which were responsible for the command and control of ISS until the more comprehensive US Laboratory arrived in February 2001 as part of 5A assembly mission. The US Lab contained the electrical, computer, and life support systems necessary to maintain the station and crew members. The next assembly mission, 6A, was launched in April 2001 and delivered the Space Station Remote Manipulator System, commonly known as the robotic arm.

The ISS US Lab has three Command and Control (C&C) computers (C&C1, C&C2, C&C3). One is designated as *primary*; one is a "hot" *backup*; and one is designated as *standby*. If the *primary* MDM fails, an automatic C&C switchover to the "hot" backup occurs. Each of the three MDMs can perform any of the three roles. Originally, the *standby* MDM was planned to be powered off until needed. But during ground testing, C&C switchovers occurred more frequently than expected, so it was decided to keep the *standby* MDM powered during most operations. Internal to each C&C is a hard disk drive, the Mass Storage Device (MSD). The only other ISS MDMs that utilize a MSD are the primary and backup payload MDMs (also located in the US Lab). [11]

During the 6A mission, the *primary* MDM, C&C1, experienced a failure and control of ISS automatically switched to C&C2 as expected. Upon switchover, C&C2 experienced five MSD *inaccessible* events. To maintain operations, the ISS ground controllers

commanded C&C2 into *standby* forcing a switchover to C&C3 as the *primary* computer. Almost immediately, C&C3 MSD indicated *non-operational* and then transitioned to an indeterminate state. Although still functional, C&C3 was operating in a degraded state because it could not access any disk files. [23]

As part of recovery efforts, ground controllers performed a reset of the MSD followed by a reset of the High Rate Data Link (HRDL) communication link. Next command and telemetry capabilities were disabled and re-enabled. The expected result, an automatic switch to C&C2, did not occur. (Later review determined the failure of C&C2 to switchover to *primary* was because it had previously been commanded to *standby*) At this point, communication with all three C&Cs (and ISS for that matter) was thought to be lost. (Note: Voice communication with the crew was still available; however, the crew had no additional visibility into the problem because the crew computer also depended on the C&C for data.) [23]

Telemetry was lost for approximately 12 to 18 hours, excluding brief time periods when ISS passed over a Russian ground station. The state of the three C&Cs was unknown and ground controllers made repeated attempts to restore the telemetry link. The command link was verified to be functional by performing a "light" test. (Commands were sent to turn on and off the ISS interior lights and ground controllers were able to utilize the video downlink to verify the lights turned on and off as commanded.) Once the command link was verified to be operational, ground controllers commanded C&C3 to power down and C&C2 transitioned to *primary*. When the crew awoke, they connected a laptop to the C&Cs and verified a valid Orbiter Interface Unit (OIU) data path. Data also indicated C&C2 had transitioned to *diagnostic*. [23]

At some point, an automated safing function on the Node MDMs called "Mighty Mouse" initiated. During "Mighty Mouse", the Node 1 MDMs take over if they think the three redundant US Lab C&Cs have failed. Once "Mighty Mouse" was initiated, the Node 1 MDMs followed a pre-prescribed sequence to reestablish control on the C&Cs. Mighty Mouse first unsuccessfully attempted to establish C&C3 as *primary*, followed by C&C1,

which was also unsuccessful. Finally, C&C2 was successfully enabled as the *primary* control computer. [23]

Communication between ISS and ground controllers was reestablished; however, the states in which the MDMs were found were unexpected. Specifically, telemetry from the on-board laptop indicated the Node MDMs were in *diagnostic*, C&C1 was *failed*, C&C3 was in *diagnostic*, and C&C2 was *primary*. Further investigation uncovered an out-of-sync timing issue between the Node MDMs and the ISS Guidance Navigation and Control (GN&C) computer had occurred causing them to transition to *diagnostic*. The Node Control Software (NCS) also had unexpectedly shutdown the Direct Current-to-Direct Current Converter Unit (DDCU), which caused the loss of one Node MDM. Additionally, an unknown event had occurred triggering a default power load shed file on C&C2. The load shed turned off the station lights, the Utility Outlet Panels, wall heaters, and Power Control Units. [23]

Recovery efforts continued but additional problems occurred. A successful Dynamic Random Access Memory (DRAM) load of C&C3 was completed but a C&C2 MSD *inaccessible* flag appeared near the end of the load. Ground controllers sent a command to reset the C&C2 HRDL, which then operated nominally through the afternoon. Later that day, second and third C&C2 MSD *inaccessible* flags were set. In parallel, the C&C1 MDM was replaced with the backup payload MDM and reloaded with C&C software. The "new" C&C1 was successfully re-initiated. Finally, ISS was able to return to normal operations. [23]

C&C3 was replaced with an MDM built from on-board spares. The failed MDMs were brought back to the ground for additional troubleshooting and investigation. Hardware damage was found on both MSDs. The cause of the damage was never determined. In order to prevent a similar incident in the future, all hard disk MSDs were replaced with Solid State Mass Memory Units (SSMMU). [24]

3.3.1.2 ISS 6A On-Orbit Anomaly Causal Factors

A full fault tree was developed as part of the problem resolution efforts but all paths could not be completely followed due to the inability to collect sufficient data. As a result, many potential causes were neither exonerated nor confirmed. [26] The official problem report stated the most probable cause was [24, pg. 1, 2]:

- C&C1: "MSD hard failed. The C&C1 MSD was not spinning post transition to *failed* state, which was confirmed by the HRDL SRAM [Static Random Access Memory] data. The root cause of hard failure is not known."
- C&C2: "MSD inaccessible state resulted from SCSI [Small Computer System Interface] Interface breakdown in HRDL during ZOE [Zone of Exclusion]." This was a known condition.
- C&C3: "MSD hard failed. Data indicated C&C3 transitioned into an already failed MDM. The root cause of the hard failure is not known."

The significance of a simultaneous failure of all three C&Cs was not ignored in the ISS risk management plan. The ISS risk management system (FMEA PRIME-7176.001) states "if all three C&C MDMs are lost, loss of ISS station-level command and control and communications and tracking system control [will occur]. Critical ISS function will be lost including communications and tracking system control and failure management, control bus MDM redundancy management, response to ISS emergencies and system-level anomalies, and caution and warning. ISS and crew may be lost." [24, pg. 2]

The probability of losing all three C&Cs simultaneously, however, was considered very unlikely and the risk was believed to be mitigated successfully through the design of three redundant computers. Unfortunately the computers were the same type and operated the same software and a similar failure occurred on two of the three computers. An additional unrelated (but known) problem on the third computer created the unlikely event of simultaneously losing all three C&C computers. A secondary recovery procedure ("Mighty Mouse") existed but also experienced an unanticipated (but known) problem.

Indications of MSD and HRDL problems were prevalent during both the standalone US laboratory ground testing and the Multi-Element Integration Test (MEIT) ground testing. One of the original payload MDMs was replaced due to a bad MSD. Several C&C switchover problems, cases of a C&C transitioning to *diagnostic* unexpectedly, and cases of a MDM not coming up MSD *functional* after a switchover occurred during ground testing. Each time a problem was found and a fix was implemented, testing continued only to have another problem surface. It was like "peeling an onion". Each new problem had been hidden by the previous problem. In hindsight, the team wondered if multiple symptoms of the same problem with the MSDs were surfacing. [11]

Chapter 4: Major Themes of In-Flight Anomaly Investigations

"If changes are to be made late in the flow, then it is imperative that the control board and project management stress the need for an understanding of the system-wide implications of the change."

- TSS-1 Investigation Board [1, pg. 45]

4.1 Introduction

The immediate cause of each in-flight anomaly discussed in the previous chapter was a technical failure; however, underlying system issues contributed to project risk creating a situation in which the technical failure occurred. This chapter presents several themes uncovered during analysis of the in-flight anomalies.

4.2 System Perspective

The primary theme found throughout accident investigation literature including the four in-flight anomalies was the absence of a holistic approach to project risk. Factors such as organizational structure, discipline bias, operational constraints, employee experience, and external pressures are often overlooked when determining project risk, yet, each directly affects project outcome. By embracing a system perspective, awareness of potential risk is extended beyond traditional technical aspects into the environment of the project itself.

For the purpose of this research, the following definition is used for *system*. A *system* is "a collection of things or elements which, working together, produce a result not achievable by the things alone." [20, pg. 295] At the system level, attributes not evident at the component level emerge as a property of the system itself. The field of system engineering evolved as a means to manage system level issues and concerns. *System engineering* is defined as "a multidisciplinary engineering discipline in which decisions and designs are based on their effect on the system as a whole." [20, pg. 295] Still, traditional risk management systems often do not address these emergent systems properties. If in addition, a holistic perspective of the project does not exist, the

associated risks can be missed. Factors effecting system perspective as manifested in the cases studies are discussed in the following sections.

4.2.1 Organizational Stovepipes

The LITE-1 in-flight anomaly was a clear example of a failure due in part to organizational stovepipes. As discussed earlier, the LITE-1 payload utilized a differential signal design that depended on equal cable lengths between the experiment and the HDRR. LITE had no reason to suspect the Shuttle Program would chose a cable that would not work with a differential design since the HDRR provided for that option. Likewise, the Shuttle Program was most likely unaware of the necessity of equal cable lengths because their responsibility ended at the standardized orbiter interface. Both groups were working in isolation, unaware of the effects the decisions they made would have on the other.

Organizational stovepipes occur when groups within a project are isolated from each other with little or no direct communication between them. If a strong system engineering function is not in place to compensate for the lack of interaction, assumptions and biases contribute to the potential for misinterpretation of requirements. Stovepipes not only exist between traditional engineering disciplines (e.g., electrical, thermal) but also appear between operational groups (e.g., ground operations, flight operations), geographical locations (e.g., KSC, JSC), and program components (e.g., shuttle, payload, ISS). Strong, ingrained stovepipes contribute to intense loyalties to one's own group and appear in such symptoms as the "not invented here" perspective or "operating with blinders on" decision making.

4.2.2 Aggregated Risk

The TSS-1 satellite failed to deploy due to interference between the tether and a bolt. The bolt was part of the wedge block modification installed late in the processing flow. The decision of the TSS-1 project to implement the less than ideal wedge block solution was attributed to the late discovery of the negative safety margin along with schedule pressure from the subsequent shuttle launch. Unfortunately, the drawings used to verify

the feasibility of the wedge block installation did not match the deployer system flight configuration and, more importantly, did not depict the proper angle to show interference between the bolt and tether. The decision to not update the drawings was most likely due to budget constraints. In addition to these factors, the deployer system was not fully tested after the installation of the wedge block modification. Individually, each of these factors probably would not lead to the on-orbit failure, but the cumulative effect compromised the checks and balances of the risk management plan. The end result was the in-flight anomaly.

Aggregated risks result from the accumulation of individual risks taken by project components on a daily basis. Each risk might have no effect on the overall project success when taken individually; but, when added to another risk, the potential for negative consequences increases. Aggregated risk may be the most difficult to mitigate because each risk aspect seems small and unrelated to another or overall mission success. Long term projects have a particular challenge. A small risk taken at the beginning of the project might not have an effect until near the end when it has potentially been forgotten or dismissed.

4.2.3 Operational Environment

The LITE/HDRR in-flight anomaly was unexpected because the interface had worked successfully during ground testing in what was believed to be flight configuration. Post-mission troubleshooting indicated the on-orbit temperature was not simulated during ground testing and the effect of temperature on LITE/HDRR operations was not fully appreciated. For the TSS-1R mission, the tether separation anomaly was most likely a result of a pinhole in the tether insulation. The sensitivity of the tether insulation to debris was not fully appreciated and the ability of the compression forces of the wind mechanism to force debris into the tether insulation was not understood.

Misconceptions about the environment in which the project will operate increase the potential for project failure. Operational environment and system design specifications are interrelated. Lack of understanding of the environmental conditions a system will

experience can lead to an inadequate design to handle such conditions. Additionally, operating a system in an environment beyond its design parameters can render a good design worthless.

4.2.4 Testing

The TSS-1 post-mission investigation board believed limitations in the test program contributed to the in-flight anomalies. Ground testing did not adequately simulate the on-orbit environment experienced by the satellite; therefore, contingency plans to address the true operational problems encountered during the mission were not accurate. Additionally, the board stressed the importance of pursuing off-nominal testing for areas of high sensitivity and high operational uncertainty such as a slack tether condition. Finally, the decision to not perform a re-test of the deployer system after the installation of the wedge block modification was a major oversight.

A comprehensive test program ideally embraces the philosophy of "fly as you test, test as you fly." In other words, testing should accurately duplicate system operations including a close approximation of the operational environment. Unfortunately, simulation of the environment of space is not always possible during ground testing. Temperature levels cannot always be replicated due to condensation concerns. Microgravity is difficult to recreate on Earth. Increased system complexity limits the ability to thoroughly reproduce operational scenarios. Budget or schedule constraints can also result in the elimination of testing that is seen as desirable but not mandatory.

4.2.5 Communication

The change from the original equal length cable harness to the 40 foot delta cable harness was not communicated to LITE through either official or unofficial channels. If LITE had been informed about the impending change, they could have shown the negative impact a cable length delta would have had on HDRR operations. A KSC engineer learned of the cable length delta during test configuration development and was unsuccessful in communicating his concern to LITE. If his concern had been effectively communicated, LITE could have requested a change back to the original equal length

cable harness or an adjustment to the length of the one cable in the new harness. Insufficient communication enabled the LITE HDRR in-flight anomaly.

The importance of effective communication across a project cannot be overstressed. Breakdowns in established communication channels as well as non-existence of crucial communication channels are the crux of accidents. Often accidents can be traced to one person knowing a critical piece of information that could have prevented or predicted the event, but that information not reaching the decision maker. Insufficient documentation on the reason behind requirements and important decisions is common. Rationale cannot be revisited or utilized for further considerations. Unsuccessful attempts to communicate concerns can lead to frustration and resignation. On the other hand, if a person repeatedly voices concerns about every detail, important or not, they can be viewed as "crying wolf" and, when the person does have a valid concern, often ignored.

4.3 Tradeoff between Low and High Risks

Three of the in-flight anomalies (TSS-1, TSS-1R, and LITE-1) occurred on missions with a high level of hazardous operations. The in-flight anomalies, however, were attributed to a non-hazardous aspect of the projects. In fact, both tether manufacturing and HDRR operations were "proven" technologies. In an effort to manage the entire project with limited resources, routine tasks or proven technologies are viewed as self-sufficient and areas of higher uncertainty receive extra scrutiny. A lesson learned from the TSS-1R board, however, stressed "there must be overt effort to assure that routine processes or actions which can violate the design intent are not overlooked." [32, pg. x]

4.4 Experimental Nature of Projects

The Spacelab/Payloads Program provided scientists and engineers the opportunity to conduct short duration experiments in the microgravity environment of low-earth orbit. The TSS and LITE missions were just that, *experiments*. Experimental projects have different types of risks. Along with the standard technical, budget, schedule, and environmental risks associated with any project, experimental projects have risks related to the uncertainties surrounding the experiment. The dynamics of a tether/deployer

system in a zero-g environment were unknown and predictions were uncertain. The feasibility of operating a high power laser in the space environment was one of the objectives of the LITE experiment. In spite of the in-flight anomalies, both projects were successful experiments. Each provided invaluable data for future missions as well as data on tether dynamics, plasma physics, and laser operations.

Chapter 5: Lessons Learned and Recommendations

"The risk management system is only as good as the engineering that informs it."

- Wayne Hale [15]

The thesis began with the desire to find the underlying causes of risk management failures in the attempt to determine lessons learned and recommendations to help future projects succeed. The official TSS-1 and TSS-1R accident reports and the LITE-1 problem report lessons learned and recommendations (available in Appendix A) are relevant to any project. Additionally, accident investigation literature provides insight into the chain of events and the less obvious causal factors of well known incidents and disasters. What became apparent as the research progressed was reasons behind accidents and the methods and tools to help prevent such disasters are well documented. Indeed, Project Management courses and textbooks discuss a multitude of techniques for risk management success. The first part this chapter discusses these key ideas, not as new or groundbreaking ideas, but as a way to reemphasis their importance.

So, the question was then raised as to why, if we already know the importance of system thinking and the affect of causal factors, do we still have such major project failures, accidents, and disasters? Why, to quote one interviewee, do we have "lessons documented [but] not necessarily learned?" [11] Although this was not the original intent of the thesis, a discussion of some factors that limit our ability to learn from our mistakes is presented. This discussion is cursory and is fruitful ground for future research topics.

This chapter concludes with recommendations to improve project and risk management approaches on future projects.

5.1 Elements of Project Success

Projects are major undertakings. Significant effort is spent procuring the time, resources, and support needed to pursue complex technical projects such as NASA's Exploration Mission to Mars. Stakeholders expect their money to be spent wisely. While nothing can

guarantee project success, research indicates the absence of key elements can set the project up for potential failure. The following paragraphs describe these key elements and offer some basic techniques that help combat the inevitable risks that arise throughout the life of a project.

5.1.1 Environmental Awareness

Major disasters often happened when less than ideal conditions align allowing undesirable events to occur. The Challenger accident and more recently the Columbia accident showed evidence of what Chiles [4] calls the "four ingredients to a really bad day":

- The situation required the machine to perform properly and flawlessly.
- The machine experienced serious problems of which there were indications under less stressful situations.
- Management was unaware of or had not followed up on reports of potential problems.
- Some natural force occurred to "tear away the facade of safety."

Of the four cases discussed in the thesis, the 6A C&C computer failures exemplify a "really bad day." The design relied on one of the three C&C computers to be operational; MSD and HRDL problems were persistent during ground testing and on-orbit operations; ground testing teams felt there was more behind the ground testing problems but their concerns were dismissed; and finally, an unknown event(s) took out two of the three computers while the third experienced another known problem at the same time.

The best risk management approaches are aware of the current environment, understand the implications of past events, and are cognizant of potential future risks. Of course, all risks cannot be eliminated in large complex technical projects. Instead, every effort is made to avoid conditions that breed mistakes and accidents. Constant vigilance prevents the need for reactionary responses and instead enables the project to proactively address

indications of impending trouble. The four ingredients of a really bad day are never allowed to combine.

5.1.2 Proficient System Engineering

The TSS-1 investigation board stressed an "aggressive and adequate SE [system engineering] assessment capability must be maintained at late stages in project cycle." [1, pg. 45] From this statement, one can infer the board believed an aggressive system engineering function would have prevented the implementation of a less than optimal technical solution for the sake of schedule. System engineering would have provided a thorough analysis of the wedge block installation and would have shown the interference that caused the tether to bind.

The role of system engineering is to provide cohesion between differing tensions as they occur throughout the project life. A robust system engineering function maintains the balance between technical, cost, schedule, and environmental factors keeping each in concert with overall project objectives. Components of a strong system engineering capability are discussed in the following sections.

5.1.2.1 Integrated Risk Management

Risk Management is often treated as an afterthought. Engineers are eager to design, regularly starting before planning is complete. Requirements are developed but the rationale behind the requirement is rarely documented. Trade studies are performed for different design elements but a detailed risk assessment is not common in the early stages of the project. Instead, contingency budget and time is set aside to handle the unexpected. The effects of the assumptions made early in the project do not arise until manufacturing, hardware integration, testing, and operations.

In the interest of maintaining a comprehensive list of risks, another common practice in large projects is for risk management to be delegated to a specific group. Different project disciplines feed their individual risks into the risk management system and the "risk" group is then responsible for tracking and statusing the risk. In effect, the

subsystems relinquish ownership of their own risks. Risk management is not seen as an integral part of engineering and instead as seen as a separate, less important and less desirable, management activity.

An integrative approach to risk management enables proactive identification of risk throughout the project life. Initial identification of risks occurs during the formulation and design phase, thus enabling early decisions to consider the potential effect on the overall risk level. Risk scenarios are periodically re-evaluated to determined if new risks have been incurred or if existing risks have increased, decreased, or been eliminated. Re-evaluation also occurs each time there is a change to the original design or plan. Additionally, unintentional emergent properties are uncovered by considering system functionality one to two layers above the component level. Aggregated risks are flushed out and system level risks are addressed. Active participation from all aspects of the project is essential during identification, evaluation, and mitigation efforts.

5.1.2.2 Continuity Across Interfaces

Problems occur at interfaces. Organizational stovepipes inhibit the flow of information between project groups. Most large projects have engineers from different companies in different geographical locations designing components that must all work together as an integrated system. Even the best written requirements, specifications, and control documents leave room for interpretation, leading to interface discrepancies.

The LITE-1 HDRR In-Flight Anomaly was partially because of assumptions about a standard interface. The shuttle design was within specifications as was the payload design. Both met the ICD; however, the delta cable length along with on-orbit temperatures produced a non-functioning design. No one looked across the payload/ shuttle interface and identified the incompatibility between the differential pair design and the HDRR-to-payload cable harness.

Documentation of rationale behind requirements as well as design and management decisions can prevent poor assumptions and misinterpretations that lead to interface

incompatibility. Another method to combat assumptions is to "follow [the] photons through instrument and spacecraft" [5] Looking across interfaces will drive out design inconsistency and requirement misinterpretation.

5.1.2.3 Comprehensive Test Program

As mentioned in Chapter 4, a comprehensive test program embraces the philosophy of "test as you fly, fly as you test." Along with standard qualification testing and interface verification testing, the expected physical and operational environment should be simulated to the highest fidelity as practical. Experience in planned and unplanned scenarios prepares the team for real time operations. Test philosophy should be established at the beginning of the project. Predefined guidelines on situations warranting retest will prevent confusion during testing activities. Adherence to and approved deviation from the established policy enables careful management of the risks associated with reduction in testing. While testing alone cannot guarantee project success, it can raise confidence in the likelihood of success. [2]

5.1.2.4 Effective Communication

Communication failure is a contributing factor in most accidents and anomalies. The change from the original cable harness to the harness with a 40 foot delta was not communicated to the LITE-1 PED at the time the decision was made. The time synchronization issue between the Node MDM and the US Lab GN&C computer prevented "Mighty Mouse" from assuming control during the 6A C&C computer anomaly. The time sync issue was a known condition but a lack of appreciation for its potential effect resulted in a non-functional contingency procedure. In both cases, had the information been effectively communicated to the right personnel, the anomalies might have been avoided.

Asking the question "Are all players represented?" during key meetings such as design and operational readiness reviews is one method to facilitate communication across a project. [28] This simple question not only identifies gaps in system representation (and thus potential areas for communication breakdown) but also emphasizes the importance

of a holistic perspective and approach to project decisions. Insisting on face-to-face communication when relaying critical information or making important decisions is another means to enhance communication. Face-to-face communication provides the sender important non-verbal feedback allowing them to know if their message is correctly received. Any miscommunication can be cleared up immediately before it has a chance to impact the project. Additionally, documentation of discussions including the rationale behind and circumstances surrounding decisions provides a historical record that can be revisited in the future when the need arises.

5.1.3 Engineering Curiosity

At the recent NASA Risk Management Council, Wayne Hale, deputy program manager of the Space Shuttle program highlighted a significant parallel between the Columbia accident and the Apollo 1 fire. Hale believed the Columbia accident was a "failure of imagination." Frank Bowman used these words when asked the cause of the Apollo 1 fire during his testimony before the Senate committee investigating the accident. [15] Both accidents were failures to imagine what could go wrong under what was considered normal operational conditions.

The best projects encourage the team to anticipate and plan for the unexpected. The simple question, "what would happen if a particular undesirable event occurred?," enables the project to prepare for what could go wrong. [4] Alternatives can be carefully considered before a crisis situation occurs. A predetermined recovery plan will save those precious few seconds before the situation goes from bad to worse. Healthy engineering curiosity also protects the project from the dangers of complacency. The loss of due diligence that complacency breeds leads to mistakes, errors, failures, and accidents. The TSS-1R investigation board believed complacency with the routine task of tether manufacturing contributed to the conditions that enabled the on-orbit tether separation. While it is expected that resources will be concentrated on the most challenging aspects of the project, care needs to be taken to ensure the simple or routine components are not overlooked or ignored. Standardized processes and procedures are one method of exacting some measure of control over routine activities; however, no

process is people proof. Project management should continue to monitor these simple aspects of the project. Trending and sampling are useful tools to watch areas that are well-known and understood.

5.1.4 Engineering Humility

Overconfidence in engineering accomplishments has been a key factor in several major accidents, most notably the Titanic disaster of 1912. The ocean liner was believed to be unsinkable. The Titanic's captain, Captain Edward John Smith, an experienced and respected captain, was quoted as saying, "Modern shipbuilding has gone beyond that [the ship sinking]." [6] Unfortunately, overconfidence in the ship design along with external pressures to achieve a speed record, adverse sea conditions, and several other contributing factors led to one of the most famous disasters of the past century.

Overconfidence can be hard to overcome, but sense of humility about what we still do not understand about complex systems can help. Projects should be wary of statements or attitudes that reflect a belief of absolute certainty. Implicit assumptions held by the project must be identified and challenged. Peer reviews and outside opinions are a valuable method to re-evaluate the mental model held by the project. The assignment of an official devil's advocate is also beneficial in challenging latent beliefs and biases. [31]

5.1.5 Hands-On Experience

Literature on the success of the Apollo program emphasizes the benefit of hands-on experience. Different terminology, journeyman, apprenticeship, hands-on training, mentoring, is used to describe this type of training. All stress the importance of new engineers getting their "hands dirty" by designing, building, testing, and operating the actual technical system. Senior NASA managers felt their hands-on experience during Apollo was a major factor in their ability to manage contractors later in their careers. As one manager commented, "no one could snow me" [22, pg. 36] because he had already experienced everything himself.

Hands-on training provides a unique opportunity to personally experience the intricacies of a complex technical project. Conducting a test highlights how different engineering components interact. Organization aspects are obvious during planning activities and project meetings. Readiness reviews expose the influences of schedule, budgetary, and environmental pressures. Because of direct involvement with day-to-day operations of the project, hands-on experience provides exposure to the broader implications of management decisions, project changes, and environmental influence. The personal experiences and lessons gained during this experience creates a more complete mental model of the system within which the project operates and a better understanding of the consequences of technical, schedule, budget, and environmental risks.

5.2 Additional Considerations

Along with the engineering challenges associated with projects, organizational cultures, human behaviors, and the dynamics of the system itself influence the potential outcome of a project. Best practices and lessons learned can help overcome some of the difficulties associated with risk management, but a more complete understanding of project challenges requires delving into the behavior of humans, systems, and their interactions. Ideas relevant to the discussion on the resistance of humans and systems to change are briefly mentioned below as topics warranting further research.

- Policy resistance, "the tendency for interventions to be delayed, diluted, or defeated by the response of the system to the intervention itself" [31, pg. 5], is inherent to systems. Policy resistance is the reason why improvements and corrections to the system often have minimal impact on overall system behavior.

- Knowledge of the reasons behind accidents is not enough to affect change. "Awareness, not knowledge, is the issue." [33] Humans hold on to their mental model in spite of evidence to the contrary. Humans believe they know what they are doing and are not aware of the true impact of their actions. As a consequence, they do not see the need to change their beliefs and behaviors. [33]

- Delays in system feedback create a barrier to learning. Humans favor short term results and have difficultly understanding long term impacts, especially in a complex system. [31]

- Changes in organizational culture are next to impossible. Examples from the implementation of lean manufacturing initiatives have shown cultural change is possible but requires a strong dedicated leader and is a slow painstaking process.

- Studies in business ethics show a significant emotional event is required to alter personal beliefs. In the absent of such an event, behavior can be altered but beliefs rarely change.

5.3 Recommendations

Along with the specific best practices discussed to address the key elements to project success, the following recommendations are provided.

- Establish a strong system engineering discipline across the agency. The importance of a system perspective must be stressed from the beginning of the project and maintained until the project is complete. A holistic perspective must be an integral part of decisions at all levels of the organization if it is expected for the line engineers to embrace it in their day-to-day activities.

- Reinstate NASA as a research and development organization. This will correctly move NASA projects out of the "pain gap". Every effort should be made to accurately portray the experimental nature of NASA projects (including the Space Shuttle, the International Space Station, and the Exploration missions to the Moon and Mars) to the agency's stakeholders. It is then the responsibility of the stakeholders to decide to what extent they choose to support NASA's vision.

- Re-establish hands-on training opportunities across the agency. New engineers should be given the opportunity to get their hands dirty through design, assembly,

and testing. Kennedy Space Center's Spacelab Experiment Integration organization (fondly called, Level IV) was an excellent model for such programs. Goddard Space Flight Center's policy of keeping at least one satellite project in-house is another good example.

- Recognize and understand the human and system factors affecting project and risk management.

- Pursue a system dynamics model approach to system safety and risk management. Current research at MIT shows promise in creating a more complete model of complex technical system behavior.

- Improve current risk management practices to include the impacts of environmental and other causal factors affecting overall project risk.

- Expand technical design philosophy to include accessibility to data critical for accident investigations. The trend over the last decade to limit (and eliminate) housekeeping data access for ground controllers leaves blind spots when trying to determine the state of the system prior to an incident. As missions become longer and more automated, visibility into the system will be crucial to understanding the state of the system at any given time.

Chapter 6: Conclusions

> *"System safety covers the total spectrum of risk management. It goes* ***beyond the hardware*** *and associated procedures of system safety engineering. It involves: attitudes and motivation of designers and production people, employee/management rapport, the relation of industrial associations among themselves and with government, human factors in supervision and quality control, documentation on the interfaces of industrial and public safety with design and operations, the interest and attitudes of top management, the effects of the legal system on the accident investigations and exchange of information, the certification of critical workers, political considerations, resources, public sentiment and many other non-technical but vital influences on the attainment of an acceptable level of risk control. These non-technical aspects of system safety cannot be ignored."*
>
> - Jerome Lederer [19, pg. 16]

6.1 Introduction

The objective of the thesis was to determine potential reasons for failure of standard risk management practices. Three Shuttle/Payloads and one ISS mission were analyzed and common factors contributing to the in-flight anomalies were identified. Key factors in project success were discussed including a cursory look at the implications of human/system behaviors. Finally, lessons learned and recommendations were provided in an effort to help future projects succeed.

6.2 Review of Hypothesis

This thesis proposed two hypotheses, both of which were confirmed.

The first hypothesis was that *anomalies, mishaps, incidents, and accidents are often caused by emergent system factors not readily apparent when combined with issues of technical failure or human error.* Each In-Flight Anomaly reviewed during this research

was traced to a technical failure. But research also indicated factors such as lack of system perspective, improper or insufficient communication, and non-technical pressures contributed as much to the environment of increased risk as the technical problem.

The second hypothesis was that *traditional tools of risk management are narrowly focused on technical, schedule, and budgetary issues and do not provide a holistic view of the true risk of the project.* All four projects used some type of risk management tool. The ISS FMEA actually contained the failure mode, but the simultaneous loss of all three C&C computers was considered highly unlikely. The redundancy of three computers was seen as adequate mitigation. Research highlights the importance of including environmental factors as well as aggregated and emergent system risks, whether using a formal system such as the risk allocation matrix or an informal list of top issues and concerns.

6.3 Summary of Findings

The major findings from the in-flight anomaly investigations and from literature review are.

- The best project management and risk management approaches incorporate several key elements:
    - A *system perspective* is embraced across the project.
    - A *comprehensive test program* is developed and valued.
    - *Communication* channels are viable and effective.
    - The risk management system adequately addresses *routine aspects* of the project.
- Best practices to counter common risk management issues and lessons learned from past incidents are well documented.
- Complex system interactions and human behavior limit the ability to learn from past mistakes and accidents.

6.4 Summary of Recommendations

Recommendations to improve the risk management and therefore the project management capability of a project have been discussed throughout the thesis and are summarized below:

- Establish a strong system engineering discipline across the agency.
- Reinstate NASA as a research and development organization.
- Re-establish hands-on training opportunities across the agency.
- Recognize and understand the human and system factors affecting project and risk management.
- Pursue a system dynamics model approach to understanding system safety and risk concerns.
- Improve current risk management practices to include the impacts of environmental and other causal factors effecting overall project risk.
- Expand technical design philosophy to include accessibility to data critical to accident investigations.

6.5 Future Research

In order to better understand the challenges of effective risk management, the following topics are suggested for future research.

- The benefit of hands-on experience has been advocated. Investigation into examples of hands-on training from within NASA as well as outside the industry would provide valuable data into the effectiveness of such programs.
- Collaborative research between system and human behaviors is suggested. Current risk management methodologies tend to focus on the technical aspects without consideration for human factors.
- Continued research into system dynamics modeling of system safety should be supported.

References

[1] Branscome, D. (Chairman). *Tethered Satellite System Contingency Investigation Board Final Report. NASA-TM-108704.* 1992.

[2] Britton, K. Schaible, D. *Testing in NASA Human-Rated Spacecraft Programs: How much is just enough?* Massachusetts Institute of Technology. February, 2003.

[3] Center for Systems Management. *Project Management.* NASA APPL Advanced Project Management Course Slides. CSM, 2002.

[4] Chiles, J. *Inviting Disaster. Lessons from the Edge of Technology.* HarperCollins. 2001.

[5] Day, R. *Warrant Holder Implementation/Engineering Authority: A Center Perspective.* NASA Risk Management Conference. December, 2005.

[6] "Disaster at Last Befalls Capt. Smith." *New York Times.* April 16, 1921. http://www.encyclopedia-titanica.org/item/3315/

[7] Dooling, D. *Spacelab Joined Diverse Scientist and Disciplines on 28 Shuttle Missions.* http://science.nasa.gov/newhome/headlines/msad15mar99_1.htm. March 15, 1999.

[8] Expert Interview #1, November 22, 2005.

[9] Expert Interview #2, November 22, 2005.

[10] Expert Interview #4, January 6, 2005.

[11] Expert Interview #5, January 9, 2006.

[12] Friedenthal, S. *Developing a Risk Management "Flight Simulator" for Manned Space Programs: A User Interface to a Systems Dynamic Simulation of System Safety at NASA.* Massachusetts of Technology. February 2006.

[13] Gerstenmaier, W. *Implementation of the Agency Strategies to Support Exploration.* NASA Risk Management Conference. December, 2005.

[14] Geveden, R. *The Fourth Element of Risk.* NASA Risk Management Conference. December, 2005.

[15] Hale, W. *Space Shuttle Program: Managing the Risks of Return to Flight.* NASA Risk Management Conference. December, 2005.

[16] Hambien, L. P. *LIDAR In-Space Technology Experiment (LITE). Mission Evaluation Report. JSC-26892.* NASA. January 1995.

[17] Leveson, N. *A New Accident Model for Engineering Safer Systems.* Massachusetts Institute of Technology. Safety Science. Vol. 42, No. 4. April 2004.

[18] Leveson, N.G. Barrett, B. Carroll, J. Cutcher-Gershenfeld, J. Dulac, N. Zipkin, D. *Modeling, Analyzing, and Engineering NASA's Safety Culture.* Phase 1 Final Report. Massachusetts Institute of Technology, 2005.

[19] Leveson, N.G. Dulac, N. Barrett, B. Cutcher-Gershenfeld, J. Friedenthal, S. *Risk Analysis of NASA Independent Technical Authority.* Massachusetts Institute of Technology. June, 2005.

[20] Maier, M. W. Rechtin, E. *The Art of Systems Architecting.* Second Edition. CRC Press. 2002.

[21] Marshall, L. Geiger, R. *Deployer Performance Results for the TSS-1 Mission. NASA-CR-202595.* NASA.

[22] McCurdy, H. *Inside NASA. High Technology and Organizational Change in the US Space Program.* The John Hopkins University Press. 1993.

[23] NASA. *50K Foot Chain of Fault Events.* (Mission Evaluation Room PowerPoint briefing.) NASA. April 30, 2001.

[24] NASA. *IFI MER-00368. C&C MSD Issues.* NASA. 2002.

[25] NASA. *IPR 63V-0001/PR SL-LITE-01-0033.* (Post-Flight Troubleshooting Problem Report for HDRR In-Flight Anomaly, IFA PYLD 07). Kennedy Space Center. September 16, 1994.

[26] NASA. *ISS Problem Report 2776: C&C 1 MDM HRDL/MSD in No-Op State.* NASA. 2002.

[27] NASA. *Risk Management Procedures and Guidelines w/ Change 1 (4/13/04), NPR 8000.4.* NASA. April 25, 2002.

[28] O'Connor, B. *Safety, Risk in the New Vision.* NASA Risk Management Conference. December, 2005.

[29] Poudrier, J. http://microgravity.hq.nasa.gov/general_info/cooperation_lite.html. October 12, 2002.

[30] Project Management Institute. *A Guide to the Project Management Body of Knowledge. 2000 Edition.* Project Management Institute. 2000.

[31] Sterman, J. *Business Dynamics. Systems Thinking and Modeling for a Complex World.* McGraw-Hill. 2000.

[32] Szalai, K. (Chairman) *TSS-1R Mission Failure Investigation Board Final Report.* NASA. May 31, 1996.

[33] Taylor, W. *Products from Complex Systems Integration: Notes from the Front Lines.* SDM Alumni Conference. October 2005.

Appendix A: Official Lessons Learned and Recommendations

TSS-1 In-Flight Anomalies

Marshall, L. Geiger, R. ***Deployer Performance Results for the TSS-1 Mission. NASA-CR-202595.*** **NASA.**

"The key lesson learned is that post-test modifications produce a significant risk in ensuring a successful mission. Ideally, testing should always be performed following hardware modifications."

Branscome, D. (Chairman). ***Tethered Satellite System Contingency Investigation Board Final Report. NASA-TM-108704.*** **1992.**

CHAPTER VIII - LESSONS LEARNED
"1. Every effort should be made to fully analyze Spacelab Carrier to satellite system (e.g. TSS-1) integrated/coupled loads prior to the Shuttle Verification Loads Analysis Cycle. The failure of the Spacelab Carrier to Tethered Satellite System structural and loads analysis processes in discovering the structural negative margins of safety resulted in a much later discovery during the Shuttle Verification Loads Analysis Cycle. The parallel developments of the EMP and TSS by separate organizations and contractors likely contributed to the failure to identify the structural negative margin of safety much earlier.

2. Ground testing should fully explore the dimensions of the expected flight environment. When hardware operation is anticipated to be sensitive to a parameter (slack tether for the TSS-1 mission), ground testing should include the inducement of off-nominal conditions related to the parameter (the inducement of slack tether in the case of the TSS-1 mission).

3. Flight hardware changes incurred late in the project cycle (in particular after completion of systems test) are at best a high risk undertaking. When "necessary" changes are made the engineering assessment and change board process must place increased emphasis on the systems implications of the change and avoid being drawn into a narrow discipline oriented process. This is particularly true when changes are being made a location geographically adjacent to an operational envelop such as that required by a translational level-wind mechanism. An aggressive and adequate systems engineering assessment capability must be maintained at late stages in a project cycle when typically the systems engineering resources available through project design are significantly reduced and the focus has changed to hardware checkout and operations. The importance of "doing it right the first time" is again reflected."

CHAPTER IX – RECOMMENDATIONS
LESSONS LEARNED
1. A critical process improvement team should be formed to review the structural and loads analyses processes and structural interface documentation currently used between the Spacelab carriers and user organizations. A specific focus should be a detailed

assessment of the process used in the conduct of the TSS-1 project, the failure to earlier identify a major structural problem within this process, and the parallel development aspects of the process.

2. Independent assessments should be required for flight hardware changes which are made after the hardware as completed systems level testing and shipped from the factory. Such assessments should emphasize the overall system implication of the changes. CAD/CAM technology and software have matured to a significant degree (particularly software associated with configuration control and the geographical relationship of components and component operational envelopes) and are commercially available. Projects should adopt this technology to facilitate systems level assessment of project design as well as systems level assessment of changes."

3. NASA as an agency, Marshall Space Flight Center, nor the contractor have specific failure policies requiring that projects pursue ground testing to off-nominal conditions. NASA as an Agency should adopt specific policies outlining criteria for projects to pursue off-nominal testing."

TSS-1R In-Flight Anomaly

Szalai, K. (Chairman) *TSS-1R Mission Failure Investigation Board Final Report.* NASA. May 31, 1996.

Lessons Learned
1. High voltage systems must thoroughly understood for electrodynamic tether applications. It is also crucial to assure that the actual operating environment matches the expected operating environment assumed by designers and developers.
2. Excellent designs can be defeated through quite common cleanliness and handling violations. There is certainly a requirement for project teams to concentrate on the most complex and challenging aspects of a systems development. There must be an overt effort to assure that routine processes or actions which can violate the design intent are not overlooked.
3. Some tests are so critical to assuring the readiness of a system for flight, that consideration should be given to repeating them as close to the mission date as practical.
4. Failure mode identification for failure modes analysis should include participation by outside specialists in the various disciplines represented by the system to assure inclusion of all critical failure scenarios."

"4.4 Recommendations
The following recommendations are applicable to reuse of the TSS-1R hardware, and to new electrodynamic tether systems developments as well. These recommendations do not apply to use of the TSS-1R deployer system for non-conducting tethers, for which the system appears to be satisfactory.
4.4.1 Manufacturing of the tether should be to rigid standards used for high voltage cables.

4.4.2 Ensure that the deployment path is free from debris
4.4.3 Reduce the possibility of arcing during tether deployment.
4.4.4 Conduct electrical integrity tests after final integration and as close to flight as possible.
4.4.5 Conduct high fidelity tests on critical subsystems to verify design or operating margins.
4.4.6 Strengthen the integrated systems development approach."

LITE-1/HDRR In-Flight Anomaly

Hambien, L. P. *LIDAR In-Space Technology Experiment (LITE). Mission Evaluation Report. JSC-26892.* NASA. January 1995.

"CORRECTIVE ACTION: During the mission the on-orbit timelines were changed to allow additional real-time science data takes through the Orbiter KU-band system. If LITE were to fly again, SMCH cables of the same lengths between data and clock pairs will be used to prevent this problem. In addition, Rockwell/Downy Design Avionics will generate a PIRN to the CORE ICD to preclude large cable length delta associated with this type of interface."

6A C&C In-Flight Anomaly

NASA. *ISS Problem Report 2776: C&C 1 MDM HRDL/MSD in No-Op State.* NASA. 2002.
"Because of that failure history, these devices are being replaced by Solid State Mass Memory Units. The MSD in C&C1 was replaced with a SSMMU on January 18, 2001. Due to the non-reoccurrence of this particular anomaly for over five months, in addition to the known failure history of the MSD and the subsequent replacement of the MSD, and the lack of any additional data to assist further investigation, this PRACA is being closed without further investigation or incurred cost."

NASA. *IFI MER-00368. C&C MSD Issues.* NASA. 2002.
"Several team working MSD and operational issues. It has been decided to replace all on-orbit MSDs (Hard Drives) with Solid State Mass Memory Units (SSMMU) circuit cards. These SSMMUs are being certified at this time and will be integrated into the program as soon as certification is complete.

Until the SSMMUs are ready to replace the MSD's on orbit, we will continue to utilize the MDM with MSDs installed. We have recommended to the Flight Control team to spin down the disk prior to powering off a MDM that has a MSD (hard drive)...

As of mission 7A.1 (8/18/01) we have three C&C MDM operational and have a complete space C&C MDM onboard should replacement be necessary."